Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

OPONENTSKÝ POSUDEK BAKALÁŘSKÉ PRÁCE

Student: **Bc. Martin Mikala** **Oponent:** **Ing. Milan Oulehla**

Studijní program: **Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**
Akademický rok: **2018/2019**

Téma bakalářské práce: **Aplikace moderních kryptoanalytických metod**

Hodnocení práce:

		A	B	C	D	E	F
		Hodnocení: A – nejlepší; F - nevyhovující					
1.	Obtížnost zadaného úkolu	☒	☐	☐	☐	☐	☐
2.	Splnění všech bodů zadání	☒	☐	☐	☐	☐	☐
3.	Práce s literaturou a její citace	☐	☒	☐	☐	☐	☐
4.	Úroveň jazykového zpracování	☐	☒	☐	☐	☐	☐
5.	Formální zpracování – celkový dojem	☐	☒	☐	☐	☐	☐
6.	Logické členění práce	☒	☐	☐	☐	☐	☐
7.	Vhodnost zvolené metody řešení	☒	☐	☐	☐	☐	☐
8.	Kvalita zpracování praktické části	☒	☐	☐	☐	☐	☐
9.	Výsledky a jejich prezentace	☒	☐	☐	☐	☐	☐
10.	Závěry práce a jejich formulace	☒	☐	☐	☐	☐	☐
11.	Přínos práce a její využití	☒	☐	☐	☐	☐	☐

Celkové hodnocení práce:
Výsledná známka není průměrem výše uvedených hodnocení. Známku uvede oponent dle svého uvážení dle klasifikační stupnice ECTS:
A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně , F – nedostatečně.
Stupeň F znamená též „nedoporučuji práci k obhajobě“.

Předloženou bakalářskou práci doporučuji k obhajobě a navrhuji hodnocení

A - výborně.

V případě hodnocení stupněm „F – nedostatečně“ uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.

Otázky k obhajobě:
Můžete vysvětlit pojem alternativní rovnice?

Kryptoanalytické metody v praktické části práce nebyly demonstrovány na symetrické šifře, která je pokládána za standardní. Jak byste popsal možnosti aplikace Vaší praktické části práce na šifru, která je definována v příloze č. 3 k vyhlášce č. 316/2014 Sb., Minimální požadavky na kryptografické algoritmy, (1) Symetrické algoritmy, a) Blokové a proudové šifry pro ochranu důvěrnosti a integrity, tedy aplikaci na Advanced Encryption Standard (AES) s využitím délky klíčů 128, 192 a 256 bitů?

Další připomínky, vyjádření, náměty k obhajobě práce (možno pokračovat i na další stránce):

Hodnocená bakalářská práce formálně i obsahově splňuje všechny body zadání. Práce má kvalitně zpracovanou teoretickou část, u které hodnotím nejen její faktickou správnost ale i přehlednost. Autor uvádí nejen samotný popis, ale je rovněž schopen i upozornit na slabá místa a omezení představených kryptografických systémů. Jedná se například o mód činnosti blokových šifer popsaný v oddíle 1.4.1 Elektronická kódová kniha (ECB - Electronic Code Book). Uvedená zjištění jsou plně v souladu se současnou odbornou literaturou. Velmi zdařile jsou rovněž zpracovány kapitoly 5 (Lineární kryptoanalýza) a 6 (Diferenciální kryptoanalýza). V praktické části kladně hodnotím skutečnost, že nebyl popsán pouze jeden typ útoku. Autor provedl útoky pomocí lineární i diferenciální kryptoanalýzy a následně provedl srovnání. Z tohoto pohledu jsou zajímavé výsledky publikované v tabulkách 11.2 až 11.5. Práce obsahuje několik drobných nedostatků jako jsou překlepy, popis rovnic, které jsou v textu uvedeny bez referencí apod. Nicméně uvedené nedostatky jsou pouze formálního charakteru a nemají vliv na odbornou kvalitu bakalářské práce.

Datum 1.6.2019 Podpis oponenta bakalářské práce